UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

WT

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
09/175,178	10/20/98	PATEL	S 13-1

EXAMINER	
NEWTON, G	
ART UNIT	**PAPER NUMBER**
2132	7

WM31/1002

LUCENT TECHNOLOGIES INC
600 MOUNTAIN AVENUE
PO BOX 636
MURRAY HILL NJ 07974-0636

DATE MAILED: 10/02/01

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary	Application No.	Applicant(s)	
	09/175,178	PATEL ET AL.	
	Examiner	Art Unit	
	Gregory A Newton	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on 7/19/01 .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-3 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-3 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 07/19/01 have been fully considered but they are not persuasive.

Applicants object to rejection of claim 1 because prime number is one prime above upper limit of Jeuneman's square hash recommendations. However, there is no rationale within specification as to why this would be a major improvement over Jeuneman's recommended range. Further more, such modifications of range do not imply patentability arguments over prior art. In regard to range modifications not implying patentability, please refer to In re Rose, 105 USPQ 237 (CCPA 1955).

Rejection of claim 2 was objected to by applicant because Takaragi's square hash function with added constant used added data rather than added keys. However, one of ordinary skill in the art would not consider adding a constant to Jeuneman's square hash as carrying patentable weight, because addition of constant offset values is well known in cryptographic art. Furthermore, please refer to third paragraph column 13 of Takaragi which states that these added values are generated by the device, which makes them not input data, but offsetting key-like data for square hash function, where offset values are well known in cryptographic art.

Rejection of claim 3 was objected to by applicants because Rohatgi hash was a summation of products as opposed to summation of squared sums. However, the modular summation of hashes was the illustrative point to be made in that one of ordinary skill in the art would have considered summation techniques in a hashing algorithm, in particular to sum square hash values of Jeuneman type. Please see enclosed added reference *Hashing by Adding*, section 5 in *A New Paradigm for Collision Free Hashing: Incrementality at Reduced Cost*, Bellare and Micciancio, Nov 96, *Advances in Cryptology, Eurocrypt 97* Proceedings.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claim 1 rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier teachings of square hash of Jeuneman.

Claim **1** recites inputting n bits, summing a key having at least n bits with the collection of bits to produce a sum, squaring the sum, and taking the result mod p, where p is first prime number greater than 2^n, and taking the final result mod 2^l , where l is less than n.

Schneier teaches on page 457 of Jeuneman's method of square hashing. Schneier does not teach of using mod prime above a range $2^n - 1$. However, examiner takes official notice that changing the range of the modular prime does not remove obviousness with respect to Jeuneman's method. Furthermore, regardless of the magnitude of the prime number, taking the result modularly will still cause overlapping values and thus no differences from Jeuneman's square hashing results. Examiner takes official notice that taking the result mod 2 to a power is well known in the art for purposes of discarding bits.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to consider the teachings in Schneier of Jeuneman's square hash with larger primes than the ones indicated in order to take advantage of larger computer capacity. One of ordinary skill in the art would have been motivated to do this by reconsidering the teachings of implications involved in limiting ranges of primes which are discussed in Schneier concerning Jeuneman's methods of square hash.

1. Claim 2 rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier teachings of square hash of Jeuneman in view of

Takaragi et al (US 6,122,375) HASH VALUE GENERATING METHOD AND DEVICE etc.

Claim **2** recites squared hash function of claim 1, except where a second key value is added to the squared quantity before taking mod p result. **Schneier** teaches on page 457 of Jeuneman's method of square hash. Schneier does not teach of adding a constant to the squared quantity before taking the modular result. However, **Takaragi** discloses e.g. in figure 11 hash function with same basic equation as claim 2. Added constant is generated by Takaragi's invention which implies it is key like data (see third paragraph column 13). Examiner takes official notice that taking the result mod two to some power is well known in the art for purposes of discarding bits.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art, upon viewing e.g. Takaragi figure 11, to combine the teachings of Schneier regarding Jeuneman's square hash with disclosures of Takaragi in order to add constants to square hash of Jeuneman. One of ordinary skill in the art would have been motivated to do this for a more secure hash with less probability of collisions.

2. Claim 3 rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier teachings of square hash of Jeuneman in view of Rohatgi (US 5,625,693), further in view of Bellare and Micciancio Eurocrypt 97 Proceedings.

Claim **3** recites summation of previously squared quantities taken mod p, then mod two to a power. **Schneier** teaches square hash function as Jeuneman's method. Schneier is silent with respect to summation of square hash terms. However, examiner takes official notice that modular summation hashes are well known in the art, and that a summation of square hash terms taken individually mod p has same result as total sum mod p. For one example of summation technique in hash function families see Rohatgi reference of note column 10.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to combine the teachings in Schneier of Jeuneman's square hash with summation techniques in order to revise hash function. One of ordinary skill in the art would have been motivated to do this for collision issues and security. (Please see: *Hashing by Adding*, section 5 in *A New Paradigm for Collision Free Hashing: Incrementality at Reduced Cost*, **Bellare and Micciancio**, Nov 96, *Advances in Cryptology, Eurocrypt 97* Proceedings.)

Conclusion

3. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Gregory A Newton whose telephone number is 703-305-1373. The examiner can normally be reached on 9-6 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tod Swann can be reached on 703-308-7791. The fax phone numbers for the organization where this application or proceeding is assigned are 703-305-0040 for regular communications and 703-305-0040 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

gn

gn
September 7, 2001